EUROPEAN DATA PROTECTION SUPERVISOR

Opinia 4/2015

W kierunku nowej etyki cyfrowej:

dane, godność i technologia

11 września 2015 r.

Europejski Inspektor Ochrony Danych (EIOD) to niezależna instytucja UE, która zgodnie z art. 41 ust. 2 rozporządzenia nr 45/2001 jest odpowiedzialna „za zapewnienie, że podstawowe prawa i wolności osób fizycznych, w szczególności prawo do prywatności są respektowane przez instytucje i organy wspólnotowe w odniesieniu do przetwarzania danych osobowych" oraz „za doradzanie instytucjom i organom wspólnotowym i podmiotom danych we wszystkich kwestiach związanych z przetwarzaniem danych osobowych". Inspektora wraz z zastępcą inspektora powołano w grudniu 2014 r., a zakres ich szczególnych kompetencji obejmował przyjęcie bardziej konstruktywnego i proaktywnego podejścia. W marcu 2015 r. EIOD opublikował pięcioletnią strategię, w której określono sposoby, w jakie zamierza zrealizować ten cel i przyjąć odpowiedzialność za te działania.

Niniejsza opinia nawiązuje do poprzedniej opinii EIOD w sprawie ogólnego rozporządzenia o ochronie danych, która miała na celu pomoc najważniejszym instytucjom UE w dążeniu do wypracowania właściwego konsensusu odnośnie do praktycznego, wybiegającego w przyszłość zestawu przepisów zapewniających ochronę praw i wolności przysługujących jednostce. Podobnie jak w opinii dotyczącej mobilnego zdrowia przedstawionej na początku 2015 r., także tym razem uwagę poświęcono wyzwaniu, jakie w kontekście digitalizacji („go digital") wiąże się z ochroną danych – trzecim z celów określonych w Strategii EIOD – polegającemu na „dostosowaniu istniejących zasad ochrony danych, aby jak najlepiej odpowiadały na potrzeby ogólnoświatowej sfery usług cyfrowych", także w świetle planów UE związanych ze stworzeniem jednolitego rynku cyfrowego. Idea ta jest spójna z podejściem Grupy Roboczej Art. 29 odnośnie do aspektów związanych z ochroną danych w związku ze stosowaniem nowych technologii, takich jak „internet przedmiotów", do którego opracowania EIOD przyczynił się jako pełnoprawny członek grupy.

Dignity	Godność
Future-oriented rules and enforcement	Zasady ukierunkowane na przyszłość i ich egzekwowanie
Accountable controllers	Odpowiedzialni administratorzy
Empowered individuals	Uprawnienia osób fizycznych
Innovative privacy engineering	Innowacyjna inżynieria uwzględniająca prywatność
Ethics	Etyka

„Godność człowieka jest nienaruszalna. Musi być szanowana i chroniona”.

Artykuł 1, Karta praw podstawowych Unii Europejskiej

Nigdy wcześniej podstawowe prawa do prywatności i ochrony danych osobowych nie były tak istotne dla ochrony godności człowieka. Zapisano je w traktatach UE oraz w Karcie praw podstawowych Unii Europejskiej. Dają one człowiekowi możliwość rozwijania własnej osobowości, prowadzenia niezależnego życia, wykazywania się innowacyjnością oraz korzystania z innych praw i wolności. Zasady ochrony danych zdefiniowane w Karcie praw podstawowych UE – konieczność, proporcjonalność, rzetelność, minimalizacja danych, ograniczenie celu, zgoda i przejrzystość – mają zastosowanie do całego procesu przetwarzania danych, tak do gromadzenia, jak i do wykorzystywania.

Technologia nie powinna narzucać wartości i praw, jednak relacji tej nie należy również sprowadzać do błędnej dychotomii. Z rewolucją cyfrową wiążą się obietnice korzyści w takich obszarach jak zdrowie, środowisko, międzynarodowy rozwój i efektywność ekonomiczna. Zgodnie z planami UE dotyczącymi stworzenia jednolitego rynku cyfrowego przetwarzanie w chmurze, „internet przedmiotów”, duże zbiory danych oraz inne technologie uznaje się za klucz do konkurencyjności i wzrostu. Modele biznesowe wykorzystują nowe możliwości w zakresie masowego gromadzenia, natychmiastowego przesyłania, łączenia i ponownego wykorzystywania danych osobowych w celach, które są niemożliwe do przewidzenia i uzasadniane długotrwałymi i mało przejrzystymi politykami prywatności. Wszystko to sprawia, że zasady ochrony danych należy rozpatrywać w obliczu nowych wyzwań wymagających świeżego spojrzenia na sposób, w jaki są one stosowane.

W dzisiejszym środowisku cyfrowym przestrzeganie prawa nie wystarcza – musimy wziąć pod uwagę wymiar etyczny przetwarzania danych. Ramy regulacyjne UE już teraz pozostawiają możliwość podejmowania elastycznych, zindywidualizowanych decyzji i określania takowych gwarancji, jeżeli chodzi o przetwarzanie danych osobowych. Dobrym krokiem naprzód będzie reforma ram regulacyjnych. Jednakże wpływ tendencji obserwowanych w opartym na danych społeczeństwie na godność, wolność jednostki i funkcjonowanie demokracji niesie ze sobą poważniejsze kwestie.

Problemy te mają implikacje natury inżynierskiej, filozoficznej, prawnej i moralnej. W niniejszej opinii wskazano niektóre istotne tendencje technologiczne, które mogą wiązać się z niedopuszczalnym przetwarzaniem danych osobowych lub naruszać prawo do prywatności. Opisano tu czteropoziomowy „ekosystem ochrony dużych zbiorów danych” stanowiący odpowiedź na wyzwanie związane z cyfryzacją – wspólny wysiłek motywowany względami etycznymi.

(1) Przyszłościowe regulacje dotyczące przetwarzania danych i poszanowania prawa do prywatności i ochrony danych.

(2) Odpowiedzialni administratorzy danych ustalający zasady przetwarzania danych osobowych.

(3) Inżynieria i projektowanie produktów i usług w zakresie przetwarzania danych uwzględniające kwestie prywatności.

(4) Uprawnienia osób fizycznych.

Europejski Inspektor Ochrony Danych zmierza do wywołania otwartej i świadomej dyskusji w ramach UE i poza jej granicami, z udziałem społeczeństwa obywatelskiego, projektantów, przedsiębiorstw, przedstawicieli środowisk naukowych, władz publicznych i organów nadzoru. Zadaniem nowej unijnej rady ds. etyki ochrony danych, którą utworzymy w ramach EIOD, będzie pomoc w zdefiniowaniu założeń nowej etyki cyfrowej, umożliwiając zyskanie większej świadomości w zakresie korzyści, jakie technologia przynosi społeczeństwu i gospodarce z dbałością o prawa i wolności osób fizycznych.

SPIS TREŚCI

1. Wszechobecność danych: tendencje, możliwości i wyzwania

Nieustannie rosnące ilości danych osobowych gromadzi się obecnie i przetwarza w coraz bardziej zawiły i złożony sposób. Wraz ze stopniowym wprowadzaniem do przedsiębiorstw i administracji publicznej komputerów w latach 80. rozpowszechniło się przekonanie, że praktyki potężnych rządów i korporacji w zakresie przetwarzania danych osobowych redukują jednostki do statusu podmiotu danych, co zagraża prawom podstawowym i wolnościom. Tym, co wyróżnia obecną falę zintegrowanej informacji i technologii komunikacyjnej, jest wszechobecność i siła.

W zeszłym roku zgłoszono, że liczba urządzeń podłączonych do internetu na naszej planecie przewyższa liczbę ludzi[1]. Wzrost odnoszący się do mocy procesorów[2], pojemności i pasm transmisji oznacza, że stopniowo ubywa technicznych ograniczeń w przetwarzaniu danych osobowych. Przewiduje się, że „internet przedmiotów" oraz analiza dużych zbiorów danych zostaną powiązane z systemami sztucznej inteligencji, naturalnego przetwarzania języka i systemami biometrycznymi w celu wyposażenia aplikacji w zdolność uczenia się maszyn na potrzeby zaawansowanej inteligencji. Rządy i spółki są w stanie wykroczyć poza „eksplorację danych" do „eksploracji rzeczywistości", która przenika nasze codzienne doświadczenie, komunikację, a nawet myśli[3]. Ponieważ społeczeństwo dostosowuje się do popytu na rynku cyfrowym, obecnie ponawiane są działania na rzecz nauczania programowania wśród dzieci[4]. Wykorzystanie tych tendencji w sektorze, w którym UE jest wiodącym konsumentem, za to pozostaje w tyle, jeżeli chodzi o świadczenie usług, to powracający motyw strategii Komisji dotyczącej jednolitego rynku cyfrowego[5].

Takie tendencje i wiele koncepcji wykorzystywanych dzisiaj, pomimo bieżącego charakteru, cechuje niejasność i nakładanie się na siebie. Aby pomóc w wywołaniu debaty, chcemy wypunktować konkretne tendencje, które choć nie wyczerpują zakresu możliwości, zwracają naszym zdaniem uwagę na najważniejsze etyczne i praktyczne zagadnienia związane ze stosowaniem zasad ochrony danych.

1.1 Duże zbiory danych

Termin „duże zbiory danych"[6] odnosi się do praktyki tworzenia olbrzymich zbiorów informacji pozyskanych z różnych źródeł i analizowania ich, często przy pomocy samouczących się algorytmów, w celu pozyskiwania wiedzy na potrzeby podejmowania decyzji. Takie informacje to nie zawsze dane osobowe: dane generowane przez czujniki służące do monitorowania zjawisk naturalnych lub atmosferycznych, takich jak pogoda lub zanieczyszczenia, lub też do monitorowania technicznych aspektów procesów produkcji nie wiążą się ze „zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną"[7]. Tym niemniej jedna z największych wartości dużych zbiorów danych dla przedsiębiorstw i rządów wynika z monitorowania zachowań *ludzi* w ujęciu zbiorowym oraz indywidualnym i tkwi w potencjalnej zdolności przewidywania[8].

Jednym z rezultatów jest powstanie modelu przychodów firm internetowych opierającego się na śledzeniu aktywności w internecie w celu optymalizacji wartości ekonomicznej transakcji z korzyścią dla usługodawcy, nie tylko w postaci reklamy ukierunkowanej, lecz także warunków polis ubezpieczeniowych, pożyczek i innych stosunków umownych oraz ich stawek lub oprocentowania. Na rynku, na którym trwa walka o uwagę użytkowników, większość ludzi jest nieświadoma szerokiego zakresu takiego monitorowania[9]. Tego rodzaju „duże zbiory danych" należy uznać za zawierające dane osobowe, nawet gdy zastosowano techniki anonimizacji: coraz łatwiej jest wyciągnąć wnioski dotyczące tożsamości osoby,

łącząc ze sobą rzekomo „anonimowe” dane z innymi zbiorami danych, w tym informacjami publicznie dostępnymi, przykładowo na portalach społecznościowych[10]. Tam, gdzie dane są przedmiotem obrotu w szczególności między granicami i jurysdykcjami, odpowiedzialność za ich przetwarzanie rozmywa się i jest trudna do zagwarantowania lub wyegzekwowania w myśl przepisów o ochronie danych osobowych, szczególnie w sytuacji braku międzynarodowych norm.

1.2 „Internet przedmiotów”

Wiele urządzeń podłączonych do internetu jest już powszechnie w użyciu, tak jak ma to miejsce w przypadku smartfonów, tabletów, bankomatów czy automatów do dokonywania odprawy przed lotem. Przewiduje się, że do 2020 r. łączność z siecią będzie standardową funkcją, a podłączonych będzie 25 miliardów przedmiotów (w 2015 r. było to 4,8 mld), od przedmiotów związanych z telemedycyną po pojazdy, od inteligentnych liczników po całą gamę nowych – stacjonarnych i mobilnych – urządzeń wspierających inteligentne miasta[11].

Czujniki te zapewnią natychmiastowe i szczegółowe informacje, do których urzędy statystyczne i badacze nie mogą dziś dotrzeć, lecz które niekoniecznie są dokładniejsze, za to mogą potencjalnie wprowadzać w błąd[12]. Szacowane 1,8 mld połączeń motoryzacyjnych maszyna–maszyna przewidywane do 2022 r. mogłoby ograniczyć wypadki i zanieczyszczenia, zwiększając produktywność, a także autonomię osób starszych i niepełnosprawnych[13]. „Urządzenia ubieralne”, takie jak ubrania i zegarki, będą przetwarzać dane osobowe podobnie jak inne urządzenia podłączone do sieci. Będą również w stanie wykrywać zakrzepy i monitorować sprawność fizyczną oraz gojenie się ran; podłączone do sieci materiały mogłyby chronić przed ekstremalnymi warunkami, np. podczas akcji gaśniczej. Tego rodzaju urządzenia będą przekazywać dane osobowe bezpośrednio do miejsca magazynowania w chmurze powiązanego z portalami społecznościowymi i potencjalnie będą podawane do wiadomości publicznej, co pozwoli na identyfikację użytkowników oraz śledzenie zachowania i ruchów poszczególnych osób oraz tłumu[14].

To, w jaki sposób informacje te są wykorzystywane może wpływać nie tylko na prywatność użytkowników urządzeń, również w sytuacji wykorzystywania ich w miejscu pracy, lecz także na prawa innych osób, które są obserwowane i rejestrowane przez urządzenie. Chociaż istnieje niewiele danych na temat faktycznej dyskryminacji, jasne jest, że olbrzymie ilości danych osobowych gromadzonych za sprawą „internetu przedmiotów” cieszą się dużym zainteresowaniem jako sposób na maksymalizację przychodu poprzez bardziej zindywidualizowaną informację cenową dostosowaną do śledzonego zachowania, szczególnie w sektorze ubezpieczeń medycznych[15]. Podważane będą również inne zasady dotyczące poszczególnych dziedzin, przykładowo gdy urządzenia wiążące się z przetwarzaniem danych medycznych nie zostaną technicznie zakwalifikowane jako wyroby medyczne i pozostaną poza zakresem zastosowania określonych przepisów[16].

1.3 Obliczenia środowiskowe

Pojęcie **obliczenia środowiskowe lub obliczenia niewidoczne** odnosi się do kluczowej technologii stanowiącej podstawę „internetu przedmiotów”. Jednym z bardziej oczywistych zastosowań są „inteligentne domy” i „inteligentne biura” składające się z urządzeń z wbudowaną zaawansowaną mocą przetwarzania informacji, co daje nadzieje na większą efektywność energetyczną i większą świadomość ludzi mogących zdalnie wpływać na poziom zużycia (chociaż będzie to zależne od poziomu niezależności mieszkańca od

właściciela lub administratora budynku). Konieczne będzie jasne określenie, kto odpowiada za cel i sposób przetwarzania danych osobowych występujących w zastosowaniach obejmujących obliczenia środowiskowe, nie tylko na potrzeby ochrony praw podstawowych osób fizycznych, lecz także na potrzeby właściwego rozdzielenia odpowiedzialności za przestrzeganie ogólnych wymogów w zakresie bezpieczeństwa systemu.

1.4 Chmura obliczeniowa

Chmura obliczeniowa jest znana jako główna technologia umożliwiająca nie tylko zaawansowaną analitykę i możliwości eksploracyjne, gromadzenie i analizę dużych zbiorów danych, lecz także przepływ danych z „internetu przedmiotów"; obecnie wykorzystywana jest przez ok. jedną piątą osób fizycznych i przedsiębiorstw w UE[17]. Pozwala ona na koncentrowanie danych z rozmaitych urządzeń wykorzystujących „internet przedmiotów", a opiera się na dostępności olbrzymich ilości danych przechowywanych w działającej na szeroką skalę infrastrukturze do przechowywania i przetwarzania danych na całym świecie, oraz na łączności z takimi danymi[18]. Szacuje się, że szersze zastosowanie chmury obliczeniowej[19] przez sektory prywatne i publiczne wniesie do PKB UE-28 dodatkowe 449 mld EUR (0,71% całkowitego PKB UE).

Kontrola danych osobowych jest często rozdzielona między klienta a dostawcę usług oferowanych w chmurze, a odpowiedzialność za realizację obowiązków związanych z ochroną danych nie zawsze jest jasna. W praktyce może to oznaczać niedostateczną ochronę. Tego rodzaju obowiązki są niezależne od **fizycznej lokalizacji miejsca przechowywania danych. Ponadto** nawet jeżeli jest to tylko technologia dodatkowa wspierająca zastosowania biznesowe, infrastruktura służąca do przetwarzania w chmurze może sama w sobie stanowić infrastrukturę newralgiczną i zwiększać nierówności w pozycji rynkowej, zważywszy że 30% przedsiębiorstw ma rzekomo trudności z rezygnacją z abonamentu lub zmianą dostawcy[20].

1.5 Modele biznesowe zależne od danych osobowych

Omawiane technologie umożliwiły powstanie nowych modeli biznesowych bazujących na informacjach generowanych nie tylko w drodze świadczenia usług, lecz również pochodzących z innych źródeł, takich jak media społecznościowe, w celu oceny ryzyka i zdolności kredytowej oraz maksymalizacji przychodu. Dominującym dziś modelem biznesowym są platformy kontaktujące sprzedawców i kupujących, umożliwiające udostępnianie i redystrybucję produktów, usług, umiejętności i zasobów. Platformy, często określane mianem platform „gospodarki współdzielenia", „zbiorowej konsumpcji" lub internetowych bądź mobilnych platform biznesowych peer-to-peer[21], mogą oferować klasyczne usprawnienia ekonomiczne, zwiększać konkurencyjność na rynku i ograniczać marnotrawienie. Szacuje się, że ich wartość globalna wzrośnie w nadchodzących latach czterokrotnie – z 26 do 110 mld USD[22]. Tego rodzaju modele biznesowe oparte na danych już teraz generują olbrzymie przychody w dziedzinie wspólnego korzystania z samochodów i najmu domów, jak również w technologii finansowej i pożyczkach społecznościowych. Badania pokazują, że konsumenci doceniają ich wyraźnie większą przystępność cenową i wygodę[23].

Walutą tego rodzaju platform jest zazwyczaj reputacja użytkownika, oceny innych użytkowników oraz weryfikacja tożsamości. Potencjalnie może to być postrzegane jako zwiększające przejrzystość i odpowiedzialność, ale niekoniecznie dzieje się tak w odniesieniu do samych dostawców platformy. Duże podmioty działające na takich rynkach są krytykowane za rzekome zachowywanie danych dotyczących reputacji poszczególnych

użytkowników, których dotyczy dana informacja. Istnieje duże ryzyko, że jednostki mogłyby zostać wykluczone z usług na bazie reputacji ocenianej na podstawie nieprawidłowych danych, których takie osoby nie mogłyby zakwestionować lub o których usunięcie nie mogłyby się zwrócić. Poleganie na danych z wielu źródeł stawia również pod znakiem zapytania obecną w prawie UE zasadę minimalizacji danych. Zakres przyszłego oddziaływania przedstawionych oraz przyszłych modeli biznesowych opartych na technologii na jednostki i społeczeństwo wymaga ostrożnego namysłu[24].

1.6 Drony i pojazdy autonomiczne

Drony, czyli częściowo autonomiczne statki powietrzne, obecnie służą głównie do celów militarnych, ale w coraz większym stopniu są wykorzystywane na potrzeby nadzoru, tworzenia map, transportu, logistyki i bezpieczeństwa publicznego, np. opanowania pożarów lasów[25]. Zdjęcia, materiały wideo oraz inne dane osobowe gromadzone przez drony mogą podlegać wymianie za pośrednictwem sieci telekomunikacyjnych. Ich stosowanie stwarza ryzyko poważnej ingerencji w prywatność oraz zniechęcenia do wolności wypowiedzi. Pojawia się pytanie, w jaki sposób ich projektowanie i stosowanie może być skutecznie regulowane, tak aby podmioty danych mogły egzekwować swoje prawa dostępu do danych przechwytywanych przez tego rodzaju maszyny.

Jeżeli chodzi o sytuację na lądzie, pojazdy autonomiczne lub samochody bezzałogowe będą zmieniać sposób korzystania z podróży i sposób jej organizacji, a także mogą spowodować zatarcie różnicy między transportem prywatnym i publicznym. Szacuje się, że do 2035 r. w użyciu będzie 12 milionów w pełni autonomicznych i 18 milionów częściowo autonomicznych pojazdów, a Europa znajdzie się w gronie najszybciej przyjmujących takie rozwiązania[26]. Algorytmy sterujące samochodami będą odpowiadały za decyzje, które mogą dotyczyć bezpośrednio integralności fizycznej, a nawet życia lub śmierci jednostek, przykładowo w sytuacji wyboru zaprogramowanego na ewentualność nieuniknionego uderzenia. Poza oczywistą potrzebą doprecyzowania, kto odpowiada za kontrolę danych i bezpieczeństwo danych, zastosowania te wywołują szereg pytań natury etycznej.

1.7 Tendencje o potencjalnie większym i długofalowym oddziaływaniu

Przewiduje się, że **biodrukowanie 3D** obiektów organicznych z wykorzystaniem kopii komórek pacjentów i kolagenowych „bio bandaży” (a zatem danych wrażliwych w świetle prawa UE) w celu pomyślnego stworzenia szeregu żyjących komórek, wkrótce będzie możliwe[27]. Ułatwiłoby to dostęp do indywidualnie dopasowanych części ludzkiego ciała i byłoby szczególnie wartościowe w biedniejszych częściach świata i obszarach dotkniętych wcześniej konfliktem. Biodruk wywołuje oczywiste pytania dotyczące etyki medycyny, zabezpieczenia własności intelektualnej i ochrony konsumenta, ale również – jako że polega na przetwarzaniu osobistych i wrażliwych danych dotyczących zdrowia jednostki – zasad ochrony danych.

Sztuczna inteligencja, jak robotyka, odnosi się do technologicznego wymogu stosowania autonomicznych maszyn, zarówno tych stacjonarnych, jak i mobilnych. Ich zaawansowanie będzie oferować rozległy potencjał wykraczający poza obecne zastosowania. Komputery dysponujące możliwością samodzielnego uczenia się uczą się zadań poprzez rozbijanie dużych zbiorów danych z wykorzystaniem (między innymi) sieci neuronowych, które mają naśladować mózg. Badacze i spółki dążą do poprawy nienadzorowanej nauki. Już teraz algorytmy potrafią rozumieć i tłumaczyć języki, rozpoznawać obrazy, pisać artykuły informacyjne i analizować dane medyczne[28]. Media społecznościowe dostarczają szerokiego

zasobu danych osobowych skutecznie oznaczonych uprzednio przez samych użytkowników. Być może ostatnim elementem na drodze kognitywnych udoskonaleń jest zwiększenie możliwości ludzkiego mózgu, przypominające zamianę papieru lub liczydła w autonomiczne maszyny, roboty, ale chwilowo należy rozważyć szersze konsekwencje dla jednostek i społeczeństwa[29].

2. Ekosystem ochrony dużych zbiorów danych

Unia Europejska ma obecnie możliwość przyjęcia pozycji lidera w demonstrowaniu, w jaki sposób rządy, organy regulacyjne, administratorzy, projektanci, programiści i osoby fizyczne mogą wspólnie działać lepiej na rzecz wzmocnienia praw oraz kształtowania, a nie blokowania, innowacji technologicznej. Tendencje opisane w części drugiej mają zdaniem jednego z komentatorów „poszerzyć przepaść między tym, co możliwe, a tym co dozwolone prawem"[30]. W przeciwieństwie do tego, co twierdzą niektórzy, prywatność i ochrona danych to platforma zrównoważonego i dynamicznego rozwoju środowiska cyfrowego, a nie przeszkoda. Niezależne organy zajmujące się ochroną danych osobowych, takie jak EIOD, odgrywają kluczową rolę w podważaniu takich mitów i reagowaniu na rzeczywiste obawy jednostek dotyczące utraty kontroli nad swoimi danymi osobowymi[31].

Kolejna generacja danych osobowych będzie z dużym prawdopodobieństwem jeszcze mniej dostępna osobom, których takie dane dotyczą. Odpowiedzialność za kształtowanie zrównoważonego jednolitego rynku cyfrowego musi być rozproszona, ale jest również współzależna, przez co przypomina ekosystem, a to sprawia, że wymaga skutecznej interakcji programistów, przedsiębiorstw i organów regulacyjnych działających w interesie jednostki. W tej części przedstawiamy wkład, jaki mogą wnieść te cztery kluczowe grupy podmiotów.

2.1 Przepisy ukierunkowane na przyszłość

W ostatnim czasie nawoływaliśmy UE do wykorzystania historycznej możliwości uproszczenia zasad postępowania z danymi osobowymi, które to zasady pozostaną istotne dla całego pokolenia[32]. Negocjacje w sprawie ogólnego rozporządzenia o ochronie danych oraz dyrektywy dotyczącej ochrony danych w obszarze policji i wymiaru sprawiedliwości dobiegają końca, a wkrótce uwaga zostanie skierowana na przyszłość dyrektywy w sprawie e-prywatności dotyczącej komunikacji elektronicznej oraz nowego rozporządzenia regulującego sposób przetwarzania danych osobowych przez same instytucje oraz organy UE. Biorąc pod uwagę, że ekonomiczny koszt gromadzenia i przechowywania danych jest niemal niezauważalny, to organom zajmującym się ochroną danych osobowych przypadnie zadanie spójnego egzekwowania takich zasad w celu uniknięcia „pokusy nadużycia" związanej z nadmiernym przetwarzaniem danych osobowych[33].

Strategia jednolitego rynku cyfrowego uznaje powiązanie między kontrolą dużych ilości danych a pozycją rynkową. Podziela się w niej wyrażone w naszej wstępnej opinii z 2014 r. pt. „Prywatność i konkurencyjność w erze dużych zbiorów danych" przekonanie o potrzebie większej spójności między organami regulacyjnymi. Unia Europejska dysponuje już narzędziami umożliwiającymi niwelowanie braku równowagi uprawnień na rynku cyfrowym: przykładowo trwające postępowania antymonopolowe Komisji Europejskiej stanowią uznanie dominacji urządzeń mobilnych w dostępie do internetu. W istniejących ramach prawnych możliwe jest bardziej całościowe egzekwowanie przepisów, chociażby poprzez unijną platformę koordynacyjną organów nadzoru, która rozstrzygałaby, czy poszczególne przypadki mogą budzić wątpliwości pod względem zgodności z przepisami dotyczącymi konkurencji, konsumentów i ochrony danych. Na przykład:

- wymaganie większej przejrzystości cen – wyrażonych w gotówce lub w inny sposób – za usługę może dostarczać wiedzy i ułatwić analizę przypadków dotyczących konkurencji[34] oraz

- wykrywanie nieuczciwej dyskryminacji cenowej opartej na słabej jakości danych i nieuczciwym profilowaniu oraz korelacji[35].

Bardziej zacieśniony dialog między organami regulacyjnymi różnych sektorów mógłby doprowadzić do reakcji na nasilające się nawoływania do partnerstw globalnych, które mogłyby tworzyć „dobra wspólne" otwartych danych, w których dane i idee, takie jak dane statystyczne i mapy, mogłyby być przekazywane i dostępne oraz wymieniane w interesie publicznym, przy mniejszym ryzyku nadzoru, w celu nadania jednostkom większej możliwości wpływania na decyzje, które ich dotyczą[36].

2.2 Odpowiedzialni administratorzy

Odpowiedzialność wymaga wprowadzenia wewnętrznych polityk i systemów kontroli gwarantujących zgodność z przepisami i zapewniających właściwe dowody, w szczególności na potrzeby niezależnych organów nadzoru.

Opowiadaliśmy się za eliminacją biurokracji w prawie ochrony danych poprzez ograniczanie do minimum wymogów zbędnej dokumentacji w celu maksymalnego zwiększania przestrzeni dla bardziej odpowiedzialnych inicjatyw podejmowanych przez przedsiębiorstwa, wspieranych wytycznymi od organów zajmujących się ochroną danych. Zasada, w myśl której dane osobowe powinny być przetwarzane wyłącznie w sposób spójny z określonymi celami, dla których dane te zostały zgromadzone, jest kluczowa dla poszanowania zasadnych oczekiwań jednostek. Przykładowo kodeksy postępowania, audyty, certyfikacje i nowa generacja klauzul umownych oraz wiążących zasad korporacyjnych mogą pomóc w budowaniu trwałego zaufania na rynku cyfrowym. Osoby odpowiedzialne za przekazywanie danych osobowych powinny być bardziej dynamiczne i aktywne oraz odchodzić od tzw. czarnej skrzynki, a więc tendencji do tajemnicy i zawiłości praktyk biznesowych przy jednoczesnym wymaganiu większej przejrzystości od klientów[37].

2.3 Inżynieria ze świadomością prywatności

Innowacje ludzkie zawsze były produktem działań konkretnych grup społecznych i konkretnego kontekstu, zazwyczaj odzwierciedlającym społeczne normy danej epoki[38]. Tym niemniej technologiczne decyzje dotyczące projektowania nie powinny decydować o kształcie naszych interakcji społecznych i struktur naszych wspólnot, lecz raczej wspierać nasze wartości i prawa podstawowe.

Unia Europejska powinna rozwijać i promować techniki inżynieryjne oraz metody umożliwiające wdrażanie technologii przetwarzania danych w celu pełnego poszanowania godności i praw jednostki. Inżynierowie ds. systemów i oprogramowania muszą rozumieć i lepiej stosować zasady projektowania uwzględniającego prywatność przy tworzeniu nowych produktów i usług we wszystkich fazach i technologiach projektowania. Odpowiedzialność musi być podparta większym wysiłkiem badawczym i rozwojowym w zakresie metod i narzędzi gwarantujących dokładność audytów oraz służących ustaleniu zgodności z przepisami działań administratorów i podmiotów przetwarzających, takich jak „tagowanie" każdego elementu danych osobowych za pomocą „metadanych" opisujących wymogi w zakresie ochrony danych osobowych.

Rozwiązania inżynieryjne powinny dać uprawnienia jednostkom chcącym zachować prywatność i wolność poprzez zachowanie anonimowości. Unia Europejska powinna promować projektowanie i wdrażanie algorytmów, które ukrywają tożsamość i łączą dane, tak aby chronić osobę fizyczną, jednocześnie ograniczając moc przewidywania, jaką dają takie dane[39].

Musimy dzisiaj położyć podwaliny pod rozwiązanie tych kwestii poprzez zbliżenie programistów i specjalistów ochrony danych z różnych obszarów w działających na szeroką skalę sieciach, takich jak Sieć Inżynierii Prywatności w Internecie (IPEN), które przyczyniają się do owocnej międzydyscyplinarnej wymiany pomysłów i metod.

2.4 Uprawnienia jednostek

Środowisko „prosumenckie”

Osoby fizyczne nie są jedynie pasywnymi podmiotami, które wymagają ochrony prawnej zamiast wyzyskiwania. Opisywane powyżej tendencje cyfryzacji tworzą pozytywne możliwości wzmocnienia roli jednostki. Przykładowo obecnie ludzie nie tylko konsumują, lecz również produkują treści i usługi, a ponadto w coraz większym stopniu mogą być uznawani za współodpowiedzialnych – obok dostawców usług – za przetwarzanie danych osobowych, chyba że dane działanie ma miejsce wyłącznie na potrzeby „gospodarstwa domowego”[40] (koncepcja „prosumentów” pojawiła się, aby oddać taki obrót stanu rzeczy[41]). Tymczasem waluty wirtualne zapewniają użytkownikom anonimowość i obchodzenie weryfikacji transakcji przez osobę trzecią, co obniża koszt transakcji w transgranicznym dokonywaniu płatności za towary i usługi. Z drugiej strony anonimowość i międzyjurysdykcyjny (czy – jak można argumentować – *ajurysdykcyjny*) charakter takich walut wirtualnych sprawia, że jednostki są narażone na trudny do wykrycia i zbadania rynek oszustw i przestępstw. Obok obowiązków leżących po stronie organów regulacyjnych, przedsiębiorstw i inżynierów, również obywatele mają obowiązek zachować czujność, ostrożność oraz krytyczną postawę, a także podejmować świadome decyzje zarówno w internecie, jak i poza nim[42].

Zgoda

Ponadto, wbrew tradycyjnemu myśleniu, nie wszystkie zachowania ludzkie można wyjaśnić zasadami ekonomicznymi zakładającymi, że ludzie postępują całkowicie racjonalnie i są wrażliwi na zachęty ekonomiczne[43]. Ma to znaczenie z perspektywy przyszłej roli zgody osoby fizycznej na przetwarzanie danych osobowych na jej temat. W myśl prawa Unii zgoda nie jest jedyną legalną podstawą większości przypadków przetwarzania. Nawet jeżeli zgoda odgrywa ważną rolę, nie zwalnia to administratorów z odpowiedzialności za to, co robią z danymi, szczególnie gdy uzyskano ogólną zgodę na przetwarzanie danych z szerokim zakresem celów takiego przetwarzania.

Kontrola i „własność” danych

Osoby fizyczne muszą mieć prawo do zakwestionowania błędów i niesłusznych uprzedzeń wynikających z logiki zastosowanej przez algorytmy w celu ustalenia założeń i przewidywań. Przykładowo w Stanach Zjednoczonych przeprowadzono badanie niemal 3 000 sprawozdań kredytowych odnoszących się do 1 000 konsumentów i wykazano, że 26% z nich zawierało „istotne” błędy, poważne na tyle, aby wpływać na ocenę zdolności kredytowej konsumenta, a przez to koszt uzyskania kredytu[44].

Dane są często uznawane za zasób, jak na przykład ropa naftowa, który może być przedmiotem obrotu – w sytuacji idealnej – między dwiema jednakowo świadomymi stronami transakcji[45]. Klienci nie są godziwie wynagradzani za ich dane osobowe będące przedmiotem obrotu, w związku z czym niektórzy opowiadają się za modelem zakładającym tytuł własności do danych. Absolutna kontrola danych osobowych jest jednak trudna do zagwarantowania – pojawią się obawy dotyczące interesu publicznego oraz praw i wolności innych osób. Kontrola jest konieczna, ale niewystarczająca[46]. Tym niemniej ludzka godność jest zawsze jednakowa, a zgodnie z prawem UE nie można zastosować odpowiednika tytułu własności jako takiego w odniesieniu do danych osobowych, które nieodłącznie wiążą się z osobowością jednostki. W przepisach UE dotyczących ochrony danych nie ma zapisów umożliwiających jednostce zrzeczenie się takiego prawa podstawowego.

Jednym z alternatywnych rozwiązań w kwestii dawania jednostkom większej kontroli nad ich danymi oraz nad tym, kto może mieć do nich dostęp i w jakim celu, mogłoby być stosowanie składów „danych osobowych" lub „skrytek danych"[47]. Koncepcja takiej „osobistej przechowalni" wymaga mechanizmów zabezpieczających, które gwarantowałyby, że tylko podmioty, które uzyskały zezwolenie od podmiotu danych, mogłyby mieć dostęp do danych i to jedynie do tych elementów, których dotyczy zezwolenie. Składy danych osobowych byłyby najskuteczniejsze w odniesieniu do bieżących i nieustannie aktualizowanych informacji, takich jak dane geoprzestrzenne czy oznaki życia. Poza zabezpieczeniami technicznymi użytkownicy danych byliby zobowiązani do poszanowania zasad udostępniania i wykorzystywania danych. Konkurencja i możliwość zmiany usługi, z jakiej się korzysta, to jedyne najskuteczniejsze uprawnienie konsumenta umożliwiające mu wpływanie na rynek dostępnych mu usług. Udowodniono już, że zapewnienie możliwości przenoszenia połączeń, w tym identyfikatorów i informacji kontaktowych, jest potężnym czynnikiem konkurencyjności i skutecznie obniżyło ceny dla konsumentów po liberalizacji rynku telekomunikacyjnego. Możliwość przenoszenia danych, a więc faktyczna i praktyczna możliwość przeniesienia większości własnych danych od jednego dostawcy usług do drugiego, to skuteczny punkt wyjścia dla tworzenia warunków rzeczywistej możliwości dokonywania wyboru przez konsumenta

3. Godność w centrum nowej etyki cyfrowej

Ramy etyczne muszą stanowić podłoże elementów ekosystemu cyfrowego. Europejski Inspektor Ochrony Danych uważa, iż większe poszanowanie i ochrona ludzkiej godności może być przeciwwagą dla wszechobecnego nadzoru i asymetrii uprawnień, z jaką obecnie mają do czynienia osoby fizyczne. Powinno to stanowić centrum nowej etyki cyfrowej.

3.1 Godność i dane

W następstwie rewolucji przemysłowej XVIII i XIX w. ruch na rzecz praw człowieka dążył do zabezpieczenia szerokiego dobra społecznego poprzez ograniczanie przeszkód w poszanowaniu jednostki. Obecnie Unia Europejska, za sprawą Karty praw podstawowych UE, oraz w ślad za Powszechną deklaracją praw człowieka i Konwencją o ochronie praw człowieka i podstawowych wolności, uznała nienaruszalność godności ludzkiej za punkt wyjścia. Godność człowieka jest nie tylko sama w sobie prawem podstawowym, lecz również fundamentem kolejnych wolności i praw, w tym prawa do prywatności i ochrony danych osobowych[48]. Naruszenie godności może obejmować uprzedmiotowienie, w ramach którego osoba jest traktowana jako narzędzie służące do realizacji czyichś celów[49]. Prywatność stanowi nieodłączny element ludzkiej godności, a prawo do ochrony danych narodziło się w latach 70. i 80. jako sposób na rekompensatę potencjalnego naruszenia prywatności i

godności za sprawą prowadzonego na szeroką skalę przetwarzania danych osobowych. W Niemczech prawo do „samostanowienia informacyjnego" oparto na prawie do godności osobistej oraz prawie swobodnego rozwoju osobowości, ustanowionych w art. 1 i 2 niemieckiej konstytucji[50].

W XXI w. od osób fizycznych w coraz większym stopniu wymaga się jednak ujawniania znacznie większej ilości danych osobowych przez internet w celu uczestnictwa w sprawach społecznych, administracyjnych lub handlowych, a możliwości rezygnacji są coraz mniejsze. Nieomal w przypadku każdej potencjalnej czynności online koncepcja wolności i świadomej zgody jest niezwykle nadwyrężana. „Cyfrowe okruchy" spadają w każdej minucie i są łączone w celu zaklasyfikowania osób fizycznych w czasie rzeczywistym do wielu – czasami sprzecznych – profili. Profile te mogą być przekazywane w przeciągu mikrosekund bez wiedzy osób i wykorzystywane jako podstawa ważnych decyzji, które tych osób dotyczą.

Profile wykorzystywane w celu przewidywania zachowania ludzi stwarzają ryzyko stygmatyzacji, wzmocnienia istniejących stereotypów, segregacji społecznej i kulturowej oraz wyłączenia społecznego[51], a tego rodzaju „zbiorowa inteligencja" podważa indywidualne wybory i równość szans. Podobne „bańki filtrów" oraz „osobiste przestrzenie odbicia echa" mogłyby doprowadzić do zablokowania kreatywności, innowacyjności oraz wolności słowa i wolności zrzeszania się, które umożliwiły wcześniej rozkwit cyfrowych technologii.

Tymczasem trwający nadal stan wyjątkowy powodowany racją „bezpieczeństwa„ wykorzystuje się w celu uzasadniania wielowarstwowego stosowania ingerujących w prywatność technik monitorowania działań osób fizycznych[52]. Rozumienie „puszczenia w ruch mechanizmu nadzoru" wymaga przyjęcia długofalowej perspektywy postrzegania ogólnego wpływu na społeczeństwo i zachowanie.

Unia Europejska razem z państwami trzecimi musi uważnie przyjrzeć się temu, w jaki sposób można zagwarantować, aby nie było tak, że poszanowanie wartości ma miejsce jedynie na papierze, podczas gdy w cyberprzestrzeni dokonuje się likwidacji tych wartości. Unia Europejska jest obecnie w krytycznym okresie poprzedzającym masowe przyjęcie takich technologii, w którym może wbudować swoje wartości w struktury cyfrowe definiujące w przyszłości nasze społeczeństwo[53]. Wymaga to nowej oceny tego, czy potencjalne zalety nowych technologii rzeczywiście zależą od gromadzenia i analizy informacji umożliwiających identyfikację miliardów osób. Taka ocena mogłaby stworzyć dla programistów wyzwanie w postaci konieczności projektowania produktów depersonalizujących w czasie rzeczywistym olbrzymie ilości niezorganizowanych informacji, co utrudniałoby lub uniemożliwiało wyodrębnienie jednej osoby.

Uznaliśmy już, że określone przetwarzanie danych, przykładowo danych genetycznych, musi nie tylko być regulowane, ale musi też podlegać ocenie w kontekście szerszych obaw społecznych, dokonywanej chociażby przez komisje etyki. Dane genetyczne, ze względu na swój charakter, dotyczą nie tylko danej osoby, lecz również jej przodków i potomków. Dane genetyczne służą nie tylko do stwierdzenia powiązań rodzinnych; elementy odnalezione w genach danej osoby mogą także dostarczyć informacji o jej rodzicach i dzieciach, a przez to doprowadzić do podejmowania przez administratorów danych decyzji wpływających na ich szanse w życiu nawet przed ich narodzinami. Potencjalna koncentracja genetycznych danych osobowych w rękach kilku olbrzymich podmiotów ma wpływ na gospodarkę rynkową, a także na podmioty danych. Narastająca zależność od globalnych systemów gromadzenia i

analizy stałych strumieni danych mogłaby uczynić społeczeństwo i gospodarkę bardziej podatnymi na bezprecedensowe defekty bezpieczeństwa i złośliwe ataki.

Istniejące ramy prawne mogłyby zawieść, jeżeli nie wkroczymy w przyszłość z innowacyjnym myśleniem. Zwiększa się potrzeba i konieczność postrzegania podmiotu danych jako osoby, a nie tylko konsumenta lub użytkownika. Prawdziwie niezależne organy zajmujące się ochroną danych mają do odegrania istotną rolę w zapobieganiu takiej przyszłości, w której los osób zależałby od algorytmów i ich nieustannych wariacji. Organy te muszą być odpowiednio wyposażone, aby móc sprawować „obowiązek opieki" nad osobami fizycznymi i chronić ich godność w internecie. Tradycyjne koncepcje i zasady prywatności oraz ochrony danych zawierały już etyczne niuanse związane z ochroną godności, przykładowo w dziedzinie zatrudnienia czy zdrowia. Niemniej jednak dzisiejsze tendencje zapoczątkowały zupełnie nowy rozdział, w którym istnieje potrzeba zbadania, czy zasady te są wystarczająco stabilne na erę cyfrową[54]. Samo pojęcie danych osobowych prawdopodobnie zmieni się radykalnie, w miarę jak technologia w coraz większym stopniu pozwoli na odtwarzanie tożsamości jednostek na podstawie pozornie anonimowych danych. Ponadto uczenie się maszyn oraz łączenie inteligencji ludzkiej i sztucznej inteligencji podważy koncepcję praw i obowiązków jednostki.

3.2 Europejska komisja doradcza ds. etyki

Celem nie jest zarysowanie alarmującego obrazu dystopii. Dyskusje w sferze prawnej, politycznej, gospodarczej, społecznej, naukowej, a nawet religijnej,[55] już się toczą. Uproszczone podejście, które daje jednostronną przewagę zyskowi gospodarczemu lub nadzorowi na potrzeby bezpieczeństwa, prawdopodobnie nie sprawdza się wcale lepiej niż nadmiernie restrykcyjne zastosowanie istniejących przepisów hamujących innowacyjność i postęp. Europejski Inspektor Ochrony Danych proponuje w związku z tym szczegółową, szeroką i multidyscyplinarną analizę służącą przedstawieniu zaleceń i dostarczeniu wiedzy na potrzeby debaty społecznej na temat sposobu stawienia czoła omawianemu wyzwaniu technologicznemu przez wolne społeczeństwo demokratyczne.

Strategia EIOD[56] przewiduje zobowiązanie do rozwoju etycznego podejścia do ochrony danych zakładającego, iż „wykonalne, użyteczne lub przynoszące zysk nie oznacza zrównoważone" i podkreślającego „odpowiedzialność za mechaniczną spójność z literą prawa". Zamierzamy dotrzeć poza wspólnotę unijnych urzędników, prawników oraz specjalistów do spraw technologii informacyjnych i zaangażować szanowane umysły, które są w stanie ocenić średnio- i długoterminowe skutki zmian technologicznych i rozwiązań regulacyjnych. W nadchodzących miesiącach utworzymy w naszej niezależnej instytucji zewnętrzną grupę doradczą ds. etycznego wymiaru ochrony danych, która zajmie się badaniem związków między prawami człowieka, technologią, rynkami a modelami biznesowymi w XXI w.

Nasza komisja doradcza ds. etyki będzie składać się z wybranej grupy szanowanych osobistości z dziedziny etyki i filozofii, socjologii, psychologii, technologii i ekonomii, wspieranej stosownie do potrzeb przez dodatkowych ekspertów dysponujących teoretyczną i praktyczną wiedzą w obszarach takich jak zdrowie, transport i energia, interakcje społeczne i media, gospodarka i finanse, rządzenie i demokracja oraz bezpieczeństwo i nadzorowanie porządku. Osoby te zostaną zaproszone do rozważenia szerszych etycznych skutków sposobu pozyskiwania i wykorzystywania danych osobowych, a obrady z ich udziałem będą toczyć się z zachowaniem pełnej przejrzystości.

4. Wnioski: czas rozpocząć pogłębioną dyskusję

Prywatność i ochrona danych stanowią część rozwiązania, a nie problemu. Jak na razie technologia kontrolowana jest przez człowieka. Niełatwo jest dokonać precyzyjnej klasyfikacji potencjalnych zmian w podziale na dobre i złe, pożądane lub szkodliwe, korzystne lub niekorzystne, tym bardziej w sytuacji, gdy potencjalne tendencje należy rozpatrywać w kontekście. Decydenci, podmioty tworzące technologie, specjaliści ds. rozwoju biznesu oraz my wszyscy musimy poważnie zastanowić się, czy i w jaki sposób chcemy wpływać na rozwój technologii i jej stosowanie. Niemniej jednak równie istotne jest, aby UE rozważyła w trybie pilnym kwestie etyczne i miejsce godności ludzkiej w kontekście nowych technologii przyszłości.

Potwierdziła się skuteczność zastosowania zasad ochrony danych dla celów ochrony osób fizycznych i ich prywatności przed ryzykiem związanym z nieodpowiedzialnym przetwarzaniem danych. Jednakże tendencje, które dziś obserwujemy, mogą wymagać zupełnie nowego podejścia. Otwieramy zatem nową debatę odnośnie do tego, w jakim zakresie zastosowanie takich zasad jak uczciwość i legalność jest wystarczające. Kręgi zaangażowane w ochronę danych mogą odegrać nową rolę, wykorzystując istniejące narzędzia, takie jak kontrole wstępne i zezwolenia – ponieważ żadne inne organy nie dysponują narzędziami w zakresie badania takich procesów przetwarzania danych. Obserwując odbywający się z zawrotną prędkością rozwój technologii, globalnej innowacyjności i sposobów tworzenia powiązań międzyludzkich, mamy możliwość zwrócenia uwagi, wywołania zainteresowania tematem i wypracowania konsensusu.

Mamy nadzieję, że niniejsza opinia będzie stanowić podstawę do szerszej i pogłębionej dyskusji na temat sposobów zapewnienia integralności wartości UE przy jednoczesnym czerpaniu korzyści z zastosowania nowych technologii.

Sporządzono w Brukseli, dnia 11 września 2015 r.

(**podpis**)

Giovanni BUTTARELLI
Europejski Inspektor Ochrony Danych

Przypisy

[1] Źródło: GSMA Intelligence.

[2] „Prawo Moore'a", według którego liczba tranzystorów, jakie można umieścić na mikrochipie, ulega podwojeniu co 18 miesięcy, zasadniczo okazało się trafne; Moore, G.E. (19-04-1965). „Cramming more components onto integrated circuits", *Electronics*. 22-08-2011.

[3] Nathan, E., Pentland, A., „Reality mining: sensing complex social systems", *Journal Personal and Ubiquitous Computing* Vol. 10 Nr 4, marzec 2006, s. 255–268. Shoshana Zuboff w artykule pt. „Big Other: surveillance capitalism and the prospects of an information civilization" (*Journal of Information Technology* (2015) 30, s. 75–89) pisze: „W wyniku wszechogarniającego zapośredniczenia komputerowego nieomal wszystkie aspekty świata są przekazywane w nowym wymiarze symbolicznym jako zdarzenia, obiekty, procesy, a ludzie stają się widoczni, poznawalni i dostępni w nowy sposób". Zuboff przewiduje „narodziny nowej uniwersalnej architektury", którą nazywa „Big Other" – „wszechobecnie działające w ramach sieci instytucje, które rejestrują, modyfikują i są w stanie utowarowić codzienne doświadczenie, od tosterów po organizmy, od komunikacji po myśl, a wszystko to w celu wytyczenia nowych ścieżek wiodących do monetyzacji i zysku"; s. 77, 81.

[4] „BBC Micro Bit computer's final design revealed" 7.07.2015, http://www.bbc.com/news/technology-33409311(accessed 10.09.2015); „No assembler required: How to teach computer science in nursery school", *The Economist*, 1.08.2015.

[5] Żadna z dziesięciu największych pod względem kapitalizacji rynkowej spółek sektora technologicznego nie ma siedziby w UE (osiem to spółki amerykańskie, jedna znajduje się w Chinach, a jedna na Tajwanie), jeżeli przyjąć dane z rankingu PWC Global Top Ten Companies by Market Capitalisation, aktualizacja: 31 marca 2015 r.

[6] „Duże zbiory danych odnoszą się do gwałtownego wzrostu zarówno dostępności, jak i zautomatyzowanego wykorzystywania informacji: dotyczy to gigantycznych cyfrowych zbiorów danych, jakimi dysponują korporacje, rządy i inne duże organizacje, a które to zbiory następnie są analizowane na szeroką skalę (stąd nazwa: analityka) za pomocą algorytmów komputerowych; opinia 3/2013 Grupy Roboczej Art. 29 w sprawie ograniczenia celu. W sprawozdaniu Białego Domu z 2014 r. opisano „duże zbiory danych" jako „rosnące technologiczne możliwości w zakresie wychwytywania, agregowania i przetwarzania coraz większych ilości, prędkości i różnorodności danych", zob. *Big Data: Seizing Opportunities, Preserving Values*, Urząd Wykonawczy Prezydenta Stanów Zjednoczonych („Podesta-report"), maj 2014 r.

[7] Zgodnie z prawem UE „dane osobowe" oznaczają „wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej („osoby, której dane dotyczą"): osoba możliwa do zidentyfikowania to osoba, której tożsamość można ustalić bezpośrednio lub pośrednio, szczególnie przez powołanie się na numer identyfikacyjny lub jeden bądź kilka szczególnych czynników określających jej fizyczną, fizjologiczną, umysłową, ekonomiczną, kulturową lub społeczną tożsamość"; art. 2 lit. a) dyrektywy 95/46/WE. Definicja ta jest w dużej mierze porównywalna z definicjami przyjętymi przez Radę Europy w Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (znanej jako Konwencja nr 108) oraz Wytycznych OECD w zakresie ochrony prywatności i przepływu danych osobowych przez granice. Dogłębna analiza – zob. Grupa Robocza Art. 29, opinia 4/2007 w sprawie pojęcia danych osobowych, WP136.

[8] Zob. na przykład przemówienie przewodniczącej amerykańskiej Federalnej Komisji Handlu z 2014 r.: „Rozpowszechnienie urządzeń podłączonych [do sieci], gwałtownie obniżający się koszt gromadzenia, przechowywania i przetwarzania informacji oraz zdolność brokerów danych i innych osób do powiązania danych offline i online oznacza, że spółki mogą łączyć praktycznie nieograniczone ilości danych o konsumentach i przechowywać je bez ograniczeń czasowych. Stosując

analitykę predykcyjną, mogą dowiedzieć się w ten sposób zaskakująco wiele o każdym z nas"; przemówienie przewodniczącej Federalnej Komisji Handlu Edith Ramirez, *Big Data: A Tool for Inclusion or Exclusion?*, Waszyngton, 15 września 2014 r. Zdaniem Sandy'ego Pentlanda „Fizyka społeczna to ilościowa nauka społeczna, która opisuje wiarygodne, matematyczne powiązania między przepływem informacji i idei z jednej strony, a zachowaniem ludzi z drugiej strony... umożliwia nam to przewidywanie produktywności małych grup, departamentów w spółkach, a nawet całych miast". Właśnie tego „potrzeba do zbudowania lepszych systemów społecznych" (s. 4, 7) oraz do „umożliwienia (funkcjonariuszom publicznym, kierownikom sektora przemysłowego i obywatelom) wykorzystywania narzędzi bodźców sieci społecznych w celu *ustanowienia nowych norm zachowań* (s. 189) (wyróżnienie własne); Pentland, A., *Social Physics: How Good Ideas Spread: The Lessons from a New Science*.

[9] Specjalne badanie Eurobarometru nr 431 w sprawie ochrony danych z czerwca 2015 r. oraz ankieta Pew Research Panel ze stycznia 2014 r. w sprawie publicznego postrzegania prywatności i bezpieczeństwa w erze post-snowdenowskiej. Jak wynika z pewnego badania, przeciętna wizyta na jednej stronie internetowej skutkuje 56 przypadkami gromadzenia danych; Angwin, J., *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance*, 2012). W sprawozdaniu Białego Domu z 2014 r. dotyczącym dużych zbiorów danych argumentowano, że „niespotykana dotąd moc obliczeniowa i poziom zaawansowania... powodują asymetrię władzy między tymi, którzy przetrzymują dane oraz tymi, którzy dostarczają te dane umyślnie lub nieopatrznie"; „jednymi z największych wyzwań ujawnionych w przeglądzie są sposoby, w jakie analityka dużych zbiorów danych może... stworzyć tak zawiłe środowisko decyzyjne, że autonomia jednostki zostanie utracona w nieprzeniknionym gąszczu algorytmów".

[10] Jeżeli posłużyć się zawierającym publiczne anonimowe dane spisem powszechnym z 1990 r., 87% populacji Stanów Zjednoczonych można by zidentyfikować po pięciocyfrowym kodzie pocztowym w powiązaniu z płcią i datą urodzenia; zob. Ohm, P., „Broken promises of privacy: responding to the surprising failure of anonymisation", *UCLA Law Review 2010* oraz *Record linkage and privacy: issues in creating new federal research and statistical info* (kwiecień 2011 r.). DNA jest unikatowe (nie licząc przypadków bliźniąt jednojajowych) i pozostaje takie samo przez całe życie. Zawiera informacje o pochodzeniu etnicznym, podatności na choroby oraz umożliwia zidentyfikowanie innych członków rodziny. W styczniu 2013 r. badacze byli w stanie identyfikować jednostki i rodziny na podstawie anonimowych danych DNA z dostępnych publicznie genealogicznych baz danych; Gymrek, M., McGuire, A.L., Golan, D., Halperin, E. i Erlich, Y., *Science* 339, 321–324 (2013). Zob. również „Poorly anonymized logs reveal NYC cab drivers' detailed whereabouts", 23.06.2014 http://arstechnica.com/tech-policy/2014/06/poorly-anonymized-logs-reveal-nyc-cab-drivers-detailed-whereabouts/ (dostęp: 10.09.2015). Zob. również Grupa Robocza Art. 29 – opinia 04/2007 w sprawie pojęcia danych osobowych; Grupa Robocza Art. 29 – opinia 03/2013 w sprawie ograniczenia celu; Grupa Robocza Art. 29 – opinia 06/2013 w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego (ISP); oraz Grupa Robocza Art. 29 – opinia 05/2014 w sprawie anonimizacji.

[11] Źródło: Gartner.

[12] Zob. na przykład dyskusja panelowa „What is the future of official statistics in the Big Data era?" Royal Statistical Society, Londyn, 19 stycznia 2015 r.; http://www.odi.org/events/4068-future-official-statistics-big-data-era (dostęp: 10.09.2015).

[13] *Ten technologies which could change our lives: potential impacts and policy implications*, Dział Prognoz Naukowych, Dyrekcja Generalna ds. Analiz Parlamentarnych, styczeń 2015 r.

[14] Unijny program prac na lata 2016–2017 w ramach programu „Horyzont 2020" wspiera tego rodzaju działania, w tym zakrojone na szeroką skalę programy pilotażowe dotyczące kwestii prywatności i etyki.

[15] Ubezpieczenia opisano jako „model biznesowy rodzimy dla internetu przedmiotów"; „From fitness trackers to drones, how the 'Internet of Things' is transforming the insurance industry", *Business*

Insider, 11.06.2015. Pojęcie dyskryminacji cenowej w prawie konkurencji, wynikające z art. 102 Traktatu o funkcjonowaniu Unii Europejskiej zabraniającego podmiotowi dominującemu na rynku „narzucania w sposób bezpośredni lub pośredni niesłusznych cen zakupu lub sprzedaży albo innych niesłusznych warunków transakcji", budzi duże kontrowersje, zob. przykładowo Gerardin, D., Petit, N.; *Price Discrimination Under EC Competition Law: Another Antitrust Theory in Search of Limiting Principles* (lipiec 2005 r.), dokumenty robocze Global Competition Law Centre seria 07/05. Duże zbiory danych i ich (według autorów niewykorzystany) potencjał w zakresie przyspieszenia zindywidualizowanej informacji cenowej – zob. Urząd Wykonawczy Prezydenta Stanów Zjednoczonych, *Big Data and Differential Pricing*, luty 2015 r., jak również niedawno przeprowadzona analiza, która zawiera wniosek, iż indywidualizowanie informacji cenowej zasadniczo obejmuje przetwarzanie danych osobowych, w związku z czym musi odbywać się z poszanowaniem zasady przejrzystości wynikającej z przepisów w zakresie ochrony danych osobowych, która wymaga od spółek informowania o celu przetwarzania danych osobowych: spółki muszą zatem informować o tym, że indywidualizują informację cenową, jeżeli ma to miejsce. Jeżeli spółka wykorzystuje pliki cookie do rozpoznania osoby, dyrektywa w sprawie e-prywatności wymaga od spółki informowania danej osoby o celu wykorzystania plików cookie; wersja robocza tekstu autorstwa Frederika Borgesiusa pt. „Online Price Discrimination and Data Protection Law". Tekst dostępny na stronie http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2652665 (dostęp: 10.09.2015).

[16] Wyroby medyczne zdefiniowano w prawie UE w dyrektywie Rady 93/42/EWG dotyczącej wyrobów medycznych zmienionej dyrektywą 2007/47/WE Parlamentu Europejskiego i Rady z dnia 5 września 2007 r. Skutki „mobilnego zdrowia" dla ochrony danych – zob. opinia EIOD 1/2015.

[17] Według danych Eurostatu z usług przechowywania w chmurze korzysta 21% osób fizycznych i 19% przedsiębiorstw w UE.

[18] „Gdyby internet był państwem, byłby na 12. miejscu na świecie pod względem wykorzystania energii elektrycznej, plasując się między Hiszpanią a Włochami. Odpowiada to ok. 1,1% do 1,5% globalnego zużycia energii elektrycznej (według stanu na rok 2010) oraz ilości gazów cieplarnianych wytwarzanych rocznie przez od 70 do 90 dużych elektrowni opalanych węglem (o mocy 500 MW)". Natural Resources Defense Council, *Data Centre Efficiency Assessment: Scaling Up Energy Efficiency Across the Data Centre Industry: Evaluating Key Drivers and Barriers 2014*.

[19] Sprawozdanie z badania „SMART 2013/0043 - Uptake of Cloud in Europe".

[20] Źródło: Eurostat.

[21] Termin „gospodarka współdzielenia" (ang. *sharing economy)* jest krytykowany jako mylący: „The Sharing Economy Isn't About Sharing at All", Eckhardt, M.G., Bardhi, F., *Harvard Business Review*, 28.01.2015.

[22] Botsman, R., Rogers, R., *What's Mine Is Yours: How Collaborative Consumption is Changing the Way We Live*, 2011.

[23] Future of Privacy Forum, *User Reputation: Building Trust and Addressing Privacy Issues in the Sharing Economy*", czerwiec 2015 r.

[24] Zob. warsztaty z dnia 9 czerwca 2015 r. zorganizowane przez amerykańską Federalną Komisję Handlu pod hasłem „Konkurencja, ochrona konsumenta i problemy gospodarcze wywołane gospodarką współdzielenia", https://www.ftc.gov/news-events/events-calendar/2015/06/sharing-economy-issues-facing-platforms-participants-regulators/ (dostęp: 10.09.2015).

[25] Skutki wykorzystywania dronów lub zdalnie sterowanych statków powietrznych dla ochrony danych – zob. opinia EIOD w sprawie komunikatu Komisji do Parlamentu Europejskiego i Rady pt. „Nowa era w dziejach lotnictwa. Otwarcie rynku lotniczego na cywilne wykorzystanie systemów zdalnie pilotowanych statków powietrznych w bezpieczny i zrównoważony sposób", listopad 2014 r.

[26] Źródło: Boston Consulting Group.

[27] Gartner.

[28] Algorytm rozpoznawania twarzy Facebook DeepFace jest skuteczny w 97% przypadków – osiągając w ten sposób wynik lepszy niż ludzie; „DeepFace: Closing the Gap to Human-Level Performance in Face Verification", tekst opublikowany w sprawozdaniu z konferencji IEEE poświęconej wizji komputerowej i rozpoznawaniu wzorów, czerwiec 2014 r.

[29] Robo zdefiniowano jako „maszynę usytuowaną w świecie, która czuje, myśli i działa"; Bekey, G., „Current trends in robotics: technology and ethics", *Robot Ethics - The ethical and social implications of robotics*, The MIT Press2, 2012, s. 18. Szacuje się, że między 2013 a 2016 r. zostanie sprzedanych 22 mln robotów usługowych; *IRF World Robotics Report*, 2013. Sztuczna inteligencja – zob. „Rise of the Machines", *The Economist*, 9.05.2015 oraz *Pew Research Centre Internet Project 2014*. Spółka działająca w dziedzinie sztucznej inteligencji uzależniła swoje przejęcie przez wiodącą spółkę technologiczną w 2014 r. od utworzenia komisji etyki i bezpieczeństwa oraz przestrzegania zakazu stosowania sztucznej inteligencji w celach militarnych lub wywiadowczych; „Inside Google's Mysterious Ethics Board", *Forbes*, 03.02.2014.

[30] Pentland, A., *Social physics*, s. 147.

[31] Zob. przypis 9 powyżej. Pentland, A., *Social Physics* s. 153: „Wielkie postępy w opiece zdrowotnej, transporcie, energetyce i bezpieczeństwie są możliwe... główną przeszkodą w osiągnięciu tych celów są obawy dotyczące prywatności oraz fakt, iż nie mamy jeszcze porozumienia dotyczącego równowagi między wartościami prywatnymi i społecznymi". Debata wokół pandemii eboli w Afryce Zachodniej z 2014 r. ilustruje, w jaki sposób rysuje się fałszywą dychotomię między prywatnością jednostki a potrzebami społecznymi. Do tej pory choroby monitorowano, a czas ich trwania mierzono poprzez ankiety i spisy, które łatwo stają się nieaktualne i które trudno ekstrapolować, aby przewidzieć, gdzie pojawi się kolejne ognisko. Istnieją przykłady wykorzystania „dużych zbiorów danych" do monitorowania ognisk malarii w Namibii i Kenii, a w 2009 r. – do monitorowania skuteczności zdrowotnych ostrzeżeń rządowych podczas meksykańskiego kryzysu związanego ze świńską grypą. Jednym ze źródeł danych są rejestry połączeń telefonicznych, które ukazują stację bazową obsługującą rozmowę i mogą w przybliżeniu w czasie rzeczywistym pozwolić ustalić lokalizację osób oraz tego, gdzie się udają. Gromadzenie takich rejestrów nie jest ukierunkowane – nie można na tej podstawie odróżnić osób zarażonych i niezarażonych Ebolą. Szwedzka organizacja non-profit stworzyła mapę mobilności ludności w Afryce Zachodniej, ale dane te nie zostały wykorzystane, ponieważ operatorzy telefonów komórkowych nie ujawnili ich zatwierdzonym badaczom zewnętrznym, utrzymując, iż muszą mieć dyspozycję od rządów, które z kolei powoływały się na kwestie prywatności, której nie można było zagwarantować w sposób zgodny z prawem UE; http://www.pri.org/stories/2014-10-24/how-big-data-could-help-stop-spread-ebola. (dostęp: 10.09.2015)

[32] Opinia Europejskiego Inspektora Ochrony Danych 3/2015.

[33] Założenie dotyczące dużych zbiorów danych „N=wszystkie" odnosi się do ujmowania wszystkich punktów danych, a nie tylko próby, Mayer-Schönberger, V., Cukier, K., *The Rise of Big Data: How it's changing the way we think about the world*, 2013. Rada Lizbońska i Instytut Polityki Progresywnej argumentowały, że dobrobyt będzie wzrastał wraz z maksymalizacją „zagęszczenia cyfrowego", a więc „ilości danych wykorzystywanych w danej gospodarce w ujęciu *per capita*" http://www.lisboncouncil.net/component/downloads/?id=1178 (dostęp: 10.09.2015). Międzynarodowa grupa robocza ds. ochrony danych w telekomunikacji (znana jako grupa berlińska) zaproponowała odstępstwa od zasad dotyczących ochrony danych osobowych odnoszące się do dużych zbiorów danych; http://www.datenschutz-berlin.de/attachments/1052/WP_Big_Data_final_clean_675.48.12.pdf. (dostęp: 10.09.2015) Światowe Forum Ekonomiczne wezwało do koncentrowania się na wykorzystaniu, a nie gromadzeniu, oraz do odejścia od wymogu zgody na gromadzenie danych osobowych; „Unlocking the Value of Personal Data: From Collection to Usage", 2013.

[34] Zob. wstępna opinia EIOD pt. „Prywatność i konkurencyjność w erze dużych zbiorów danych".

[35] Zgodnie z art. 21 Karty praw podstawowych UE „[z]akazana jest wszelka dyskryminacja w szczególności ze względu na płeć, rasę, kolor skóry, pochodzenie etniczne lub społeczne, cechy genetyczne, język, religię lub przekonania, poglądy polityczne lub wszelkie inne poglądy, przynależność do mniejszości narodowej, majątek, urodzenie, niepełnosprawność, wiek lub orientację seksualną". Wiele z tych kategorii danych („ujawniających pochodzenie rasowe lub etniczne, opinie polityczne, przekonania religijne lub filozoficzne, przynależność do związków zawodowych, jak również przetwarzanie danych dotyczących zdrowia i życia seksualnego") jest objętych wzmocnioną ochroną na podstawie art. 8 dyrektywy 95/46/WE.

[36] Koncepcja cyfrowych dóbr wspólnych – zob. „Ambition numérique: Pour une politique française et européenne de la transition numérique", Francuska Rada Cyfrowa, czerwiec 2015 r., s. 276; Bruce Schneier opowiada się za stworzeniem w internecie „przestrzeni publicznych niczyich", przypominających parki publiczne, *Data and Goliath*, s. 188–189; Sandy Pentland opowiada się za „dobrem wspólnym danych publicznych", *Social Physics*, s. 179. Ocena bezpieczeństwa publikowania zagregowanych zbiorów danych jako otwartych danych – zob. Grupa Robocza Art. 29 – Opinia 06/2013 w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego (ISP).

[37] „Während die Einzelnen immer transparenter werden, agieren viele Unternehmen hochgradig intransparent" http://crackedlabs.org/studie-kommerzielle-ueberwachung/info. Przejrzystość kwalifikowana – zob. na przykład Pasquale, F., *The Black Box Society: The Secret Algorithms that Control Money and Information*.

[38] „Za technologią wpływającą na nasze relacje społeczne stoją dokładnie te same relacje społeczne", Noble, D., „Social Choice in Machine Design: The Case of Automatically Controlled Machine Tools", *Case Studies in the Labor Process*, red. Andrew Zimbalist, 1979. Zob. też Wajcman, J., *Pressed for Time: The Acceleration of Life in Digital Capitalism*, 2014 s. 89–90; oraz Zuboff, *Big Other* (dane bibliograficzne w przypisie 3 powyżej).

[39] Opinia 05/2014 w sprawie technik anonimizacji z dnia 10 kwietnia 2014 r. (WP 216).

[40] Wąska interpretacja wyłączenia z zasad ochrony danych na użytek czysto osobisty lub użytek gospodarstwa domowego – zob. wyrok Trybunału Sprawiedliwości Unii Europejskiej w sprawie C-212/13, František Ryneš przeciwko Úřad pro ochranu osobních údajů.

[41] Termin „prosument" został ukuty przez Alvina Tofflera w *The Third Wave*,1980. Dyskusja na temat „środowiska prosumenckiego" oraz sposobu, w jaki powinno się je regulować – zob. Brown, I., Marsden, Ch., *Regulating Code*, 2013.

[42] Opinia Europejskiej Grupy ds. Etyki w Nauce i Nowych Technologiach do Komisji Europejskiej: Etyka technologii bezpieczeństwa i nadzoru, Opinia nr 28, 20.05.2015, s. 74.

[43]Zob. przykładowo *Homer Economicus: The Simpsons and Economics*, red. Joshua Hall, 2014.

[44] Według najbardziej konserwatywnej definicji błędu oznacza to, że 23 mln Amerykanów ma w swoim sprawozdaniu o konsumencie istotne błędy. Pięć procent uczestników badania miało błędy, których poprawienie wpłynęło pozytywnie na zdolność kredytową, dzięki czemu możliwe było uzyskanie kredytu po niższej cenie; Federalna Komisja Handlu, Sprawozdanie dla Kongresu na podstawie sekcji 319 Ustawy o uczciwych i dokładnych transakcjach kredytowych z 2003 r., grudzień 2012 r., Hoofnagle, Ch.J., „How the Fair Credit Reporting Act Regulates Big Data" (10 września 2013 r.). *Future of Privacy Forum Workshop on Big Data and Privacy: Making Ends Meet*, 2013. Tekst dostępny na stronie SSRN: http://ssrn.com/abstract=2432955.

[45] WEF klasyfikuje dane jako wartościowe mienie każdej jednostki, co do których prawo do posiadania, wykorzystania i dysponowania może być udzielone spółkom i rządom w zamian za usługi. Zob. niedawne przemówienia wiceprzewodniczącego Komisji Andrusa Ansipa, przykładowo z dnia 07.09.2015 r. podczas dorocznego zebrania w Brugii pt. „Productivity, innovation and

digitalisation – which global policy challenges?": „Własność strumieni danych i zarządzanie nimi, wykorzystywanie i ponowne wykorzystywanie danych. Zarządzanie danymi i ich przechowywanie. Oto podbudowa ważnych nowo powstających sektorów, takich jak chmura obliczeniowa, internet przedmiotów i duże zbiory danych".

[46] „Kto więc ma prawo do wykorzystywania informacji i danych, które w rzeczywistości do niego nie należą? Oto zagadnienie wykraczające poza granice handlu, etyki i moralności, prowadzące do kwestii prywatności i ochrony prywatności"; Al-Khouri, listopad 2012 r., http://www.academia.edu/6726887/Data_Ownership_Who_Owns_My_Data_036. Zob. również Radin, M.J., „Incomplete Commodification in the Computerized World", *The Commodification of Information* 3, 17, red. Niva Elkin-Koren, Neil Weinstock Netanel, 2002: „Duże znaczenie ma to, czy prywatność jest postrzegana jako prawo człowieka przysługujące osobie ze względu na jej podmiotowość czy jako prawo rzeczowe, a więc to, co może być przedmiotem własności i kontroli innych osób. Prawa człowieka są z założenia niezbywalne, natomiast prawa rzeczowe z założenia podlegają zbyciu".

[47] Międzychmurowy projekt Laboratorium Nauk Komputerowych i Sztucznej Inteligencji MIT wspierany przez szereg spółek z siedzibą w UE ma na celu „1) ułatwienie rozwoju oprogramowania obejmującego wielu użytkowników („społecznościowego") z zastosowaniem jedynie programowania front-end oraz z poszanowaniem praw i prywatności użytkowników; oraz 2) umożliwienie użytkownikom łatwego przemieszczania się pomiędzy aplikacjami, platformami sprzętowymi i portalami społecznościowymi z zachowaniem danych i kontaktów towarzyskich"; http://openpds.media.mit.edu/#architecture (dostęp:10.09.2015).

[48] Zob. wyjaśnienie art. 1 Karty praw podstawowych Unii Europejskiej.

[49] Nussbaum, M., „Objectification", *Philopsophy and Public Affairs* 24, 4, 1995.

[50] Wyrok z dnia 15 grudnia 1983 r., BVerfGE 65, 1–71, Volkszählung.

[51] Zob. Europejska Grupa ds. Etyki w Nauce i Nowych Technologiach, Opinia w sprawie etyki i nadzoru, s. 75. Badanie sugeruje, że algorytm reklamy ukierunkowanej był dyskryminujący ze względu na to, iż reklamy lepiej płatnych miejsc pracy wyświetlały się częściej mężczyznom niż kobietom odwiedzającym strony z ofertami pracy; Carnegie Mellon University oraz International Computer Science Institute. Tendencja do stosowania w cyfrowych asystentach domyślnego głosu kobiecego – zob. Wajcman, J., „Feminist theories of technology", *Cambridge Journal of Economics*, 34 (1), s. 143–152, 2010.

[52] Agamben, G., *State of Exception*, 2005.

[53] Richards, N., Jonathan, K., „Big Data Ethics" (19 maja 2014 r.), *Wake Forest Law Review*, 2014.

[54] BBC, „Information watchdog investigates *charity data sales*", 1.09.2015.

[55] Zob. list od Future of Life Institute. Encyklika papieska *Laudato Si:* zawiera słowa: „Dołącza się do tego dynamika mediów i świata cyfrowego, gdy staje się wszechobecna, nie sprzyjając rozwojowi zdolności do mądrego życia, głębokiego myślenia, wielkodusznego miłowania. Wielkim mędrcom przeszłości groziłoby w tym kontekście, że będą świadkami, jak ich mądrość jest przytłumiana pośród rozpraszającego zgiełku informacyjnego. Konieczny jest wysiłek, aby środki te stały się bodźcem do nowego rozwoju kulturalnego ludzkości, a nie degradacją jej najgłębszego bogactwa. Prawdziwej mądrości, owocu refleksji, dialogu i wielkodusznego spotkania między ludźmi, nie osiąga się jedynie na drodze gromadzenia danych, prowadzącego do przesytu i zamętu w swego rodzaju skażeniu umysłowym. Równocześnie istnieje tendencja do zastąpienia realnych relacji z innymi, ze wszystkimi związanymi z nimi wyzwaniami, przez pewien typ komunikacji za pośrednictwem internetu. Pozwala to na selekcjonowanie lub eliminowanie relacji według naszego uznania. W ten sposób rodzi się nowy rodzaj sztucznych emocji, które mają więcej wspólnego z urządzeniami i ekranami niż z osobami i przyrodą. Obecne środki pozwalają nam komunikować się oraz dzielić wiedzą i uczuciami. Jednak czasami uniemożliwiają nam bezpośredni kontakt z niepokojem, wstrząsem, radością bliźniego oraz

złożonością jego doświadczenia osobistego. Nie powinno więc dziwić, że wraz z przytłaczającą podażą tych produktów narasta głęboka melancholia i niezadowolenie w relacjach międzyosobowych czy też niebezpieczna izolacja".

[56] Zob. Działanie 4 strategii EIOD na lata 2015–2020, rozwój etycznego wymiaru ochrony danych.